Financial Crime and Risk Management

cyber security FinCen

The Financial Crimes Enforcement Network (FINCEN) occasionally will issue reports around the work depository institutions and others are doing to protect the country in this area. For 2016, the data is in and you may be interested to know depository institutions filed a whopping 2.67mm suspicious activity reports (SARs). Wow.

It can be comforting to think that most financial crimes happen in big cities, at banks with international connections and vast service networks that can be compromised. Bad guys just don't waste their time laundering their loot through friendly community banks. It may seem unlikely, but when it comes to criminals, no bank is too small. Indeed, an out-of-the-way community bank might be more attractive than a big bank to these evil doers.

Fifteen years ago, the Patriot Act ushered in a new era of financial crime risk management and compliance for banks. Banks big and small devoted significant resources to that effort as the government cracked down on banks that failed to properly guard against the chance of being compromised.

Fortunately, progress has been made. In a recent report, Deloitte says that the level of enforcement actions has recently begun to decline. This might be an indication that the measures taken by banks are working, so that fewer infractions are showing up. To date, banks have been quite diligent in responding to the challenges of financial crime and the reporting demands of the Bank Secrecy Act. There is now more information available to the government to help track and pursue the assets of criminal and terrorist enterprises.

But one consequence of the heightened focus on crime risk is that some banks consciously try to avoid doing business with potentially risky customers, including those with foreign connections which might in some way seem suspicious and thus pose a potential risk. Deloitte's report notes that this type of de-risking has become so pervasive that it has begun to restrict the availability of financial services in certain counties and regions - a sort of crime-risk-based red-lining.

Knowing this, you must be vigilant yet mindful in these matters. It is important to not only ensure rogue customers are weeded out of the system, but also that genuine, potentially valuable customers are not. The government has begun looking into this situation, since de-risking may have the unintended consequence of denying financial services to customers doing legal business.

That said, community banks need to be keenly aware of the real possibility that some criminals may find themselves frozen out of big banks due to robust crime risk management systems. These larger banks actively de-risk certain customers, industries and all sorts of things in between.

As the Deloitte report further points out, criminals are constantly devising new schemes to launder money. Setting up a bank crime risk management and compliance system is important, but so is monitoring emerging challenges and updating compliance systems. Keeping up with new technology solutions for compliance and analytics can also be helpful. Lastly, remember that even with the best systems in place, a single willing

employee can cause considerable damage. So, don't forget about employee compliance training and internal checks as well.

At the end of the day, we know community bankers have put the appropriate measures in place to prevent money laundering and financial crime. We just want to remind everyone that the risk never goes away. Regulators expect banks to diligently continue checking and updating their processes and procedures, while staying aware of any new developments. A well-integrated risk management and compliance system is the best weapon in this blistering hot regulatory area so be extra diligent.